TBCC IDENTITY THEFT PREVENTION PROGRAM
ADMINISTRATIVE RULE NUMBER: B013
LAST APPROVED: April 01, 2013, January 15, 2015, February 2019
RELATED TO POLICY SERIES NUMBER: 212

PURPOSE: B013.1

This rule establishes procedures for an identity theft prevention program. The program is designed to detect, prevent and mitigate identity theft. This policy applies to college accounts or procedures which either:

A. allow a person to register, receive financial aid, make payments or be employed by the College;

B. or present a "reasonably foreseeable risk" of identity theft.

DEFINITIONS: B013.2

A covered account means:

A. A record that the College maintains primarily for registration, financial aid, accounts receivable or payable or employment; and

B. Any other record that the College maintains for which there is a reasonably foreseeable risk of Identity theft to the person or a risk to the safety and soundness of the college's records including financial, operational, compliance, reputation or litigation risks.

C. Identify theft means fraud committed or attempted using the Identifying Information of another person without authority.

D. A red flag means a pattern, practice or specific activity that indicates the possible existence of identity theft.

E. Identifying information means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, Social Security number, date of birth, government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, credit or debit card number, or account passwords.

F. Security information is defined as government data the disclosure of which would be likely to substantially jeopardize the security of identifying information.

PROGRAM: B013.3

This Identity theft prevention program is intended to help to detect, prevent and mitigate

identity theft. The program includes procedures to:

A. Identify red flags for covered records and incorporate those red flags into the program;

B. Detect red flags that have been incorporated into the program;

C. Respond appropriately to any detected red flags to prevent and mitigate identity theft; and

D. Update the program periodically to reflect changes in risks to students or employees and to ensure the safety and soundness of the College from identity theft.

PROGRAM ADMINISTRATION: B013.4

Oversight

Responsibility for developing, implementing and updating this program lies with the Director of Human Resources and the Identity Theft Committee. The Committee will be comprised of:

A. Associate Vice President of Student Services and Director of Information Technology

B. Comptroller/CFO

The Director of Human Resources and the Committee will be responsible for:

A. Program resources and planning;

B. Ensuring appropriate program training of College staff;

C. Reviewing any staff reports regarding red flag detection and Identification Theft mitigation and prevention;

D. Determining which steps of prevention and mitigation should be taken in particular circumstances commensurate with the risk posed; and

E. Considering periodic changes to the program.

The Director of Human Resources and Committee will review and as necessary, update this program at least once a year to reflect changes in risks to students or employees and the soundness of protection of College records from identity theft. In doing so, the Director of Human Resources and Committee will consider the College's experience

with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the College's business arrangements with other entities. After considering these factors, including the degree of identity theft risk posed, the Director of Human Resources and Committee will determine whether changes to the program, including the listing of new red flags, are warranted. If warranted the Director of Human Resources and Committee will update the program and present College Council with recommended changes and they will make a determination of whether to accept, modify or reject those changes to the program.

College departments that have a central role in preventing identity theft and implementing this program are: Student Services and the Business Office (including the TBCC Store). Department heads are responsible for familiarizing themselves with the program. Department heads shall meet with their respective staff members annually to assess current compliance. Staff responsible for implementing the program will be trained by or under the direction of the Committee. Staff will provide timely reports to the Committee on all incidents of identity theft or occurrences of red flags.

IDENTIFICATION OF RED FLAGS: B013.5

In order to identify red flags, the College considers the types of records it maintains, the methods it uses to open and access records, and its previous experiences with identity theft. The College has identified the following red flags in each of the listed categories:

Notifications and Warnings from Credit Reporting or Background Check Agencies

Red Flags

A. Report of fraud accompanying a credit or background report;

B. Notice or report from a credit agency of a credit freeze on a student, employee or applicant;

C. Notice or report from a credit agency of an active duty alert for an applicant;

D. Indication from a credit report of activity that is inconsistent with a student’s or employee’s usual pattern or activity.

Suspicious Documents

Red Flags

A. Identifying Information that appears to be forged, altered or inauthentic;

B. Identifying Information on which a person's photograph or physical description is

inconsistent with the person presenting the document;

C. Other document with information that is inconsistent with existing student or employee information (such as if a person's signature on a check appears forged);

D. Application material that appears to have been altered or forged.

Suspicious Personal Identifying Information

Red Flags

A. Identifying Information presented inconsistent with other information the student or employee provides (example: inconsistent birth dates);

B. Identifying Information presented inconsistent with other sources of information (for instance, an address not matching an address on file);

C. Identifying Information presented that is the same as information shown on other applications that were found to be fraudulent;

D. Identifying Information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

E. Social security number presented that is the same as one given by another student or employee;

F. Failure to provide complete personal Identifying Information on an application when reminded to do so; and

G. Identifying Information inconsistent with the information on file for the student or employee.

Suspicious Activity or Unusual Use of Account

Red Flags

A. Change of address for a record followed by a request to change the record holder's name;

B. Mail sent to the record holder is repeatedly returned as undeliverable;

C. Notice to the College that a student or employee is not receiving mail sent by the College;

D. Notice to the College that an account has unauthorized activity;

E. Breach in the College computer system security; and

F. Unauthorized access to or use of student or employee account information.

Alerts from Others

Red Flag

A. Notice to the College from a student or employee, identity theft victim, law enforcement or other person that the College has opened or is maintaining a fraudulent record for a person engaged in identity theft.

DETECTING RED FLAGS: B013.6

New Records

In order to detect any of the red flags identified above associated with a new record or which presents a foreseeable risk of identity theft, college personnel will take the following steps to obtain and verify the identity of the person or business opening the account:

A. Require certain Identifying Information, including:

    a. Full name;

    b. Date of birth (for individual);

    c. Previous and current residential or business address; and

    d. Identification. Required identification shall include the following:

        i. For a U.S. Citizen

            1. Social Security number; and/or

            2. Photo-bearing documents (original required) such as:

                a. State-issued driver's license; or

                b. State-issued identification card; or

                c. United States Passport.

        ii. For a Non-U.S. Citizen

1. Social Security number; and/or

2. Photo-bearing documents (original required) such as:

    a. State-issued driver's license; or

    b. State-issued identification card; or

    c. Passport from any country; or

    d. Documents containing an alien identification number and country of issuance; or

    e. Any other photo-bearing government-issued document evidencing nationality or residence.

B. Review all documentation for red flags; and/or independently contact the student or employee.

Existing Records

In order to detect any of the red flags identified above for an existing record, personnel will take the below steps to monitor transactions. College personnel have the discretion to determine the degree of risk posed and to act accordingly.

A. Verify a person's identifying Information if a person requests any information on the record (this can be done in person, via telephone, via facsimile, or via email);

B. Verify the validity of requests to change address; and

C. Verify changes in banking information given for payment purposes.

PREVENTING AND MITIGATING THEFT: B013.7

A. Ongoing Operations to Prevent Identity Theft. In order to further prevent the likelihood of identity theft, personnel will take the below steps, commensurate with the degree of risk posed, regarding ongoing internal operating procedures. College personnel have the discretion to determine the degree of risk posed and to act accordingly.

    a. Ensure that its website is secure or provide clear notice that the website is not secure;

    b. Ensure complete and secure destruction of paper documents and computer files containing a person’s Identifying Information;

c. Ensure that office computers are password protected;

d. Keep offices clear of papers containing personal information.

e. Ensure computer virus protection is up-to-date;

f. Require and keep only information necessary for business purposes;

g. Transmit identifying information using only approved methods and include the following statement on any transmitted identifying information:

"This message may contain confidential and/or proprietary information, and is intended for the person/entity to which it was originally addressed. If you have received this email by error, please contact the college and then shred the original document. Any use by others is strictly prohibited."

h. Do not use or post person's Social Security number as an account identifier or on any other documents unless requested by person or required by federal law (such as W-2 forms).

B. Steps to take when you detect a red flag. In the event college personnel detect red flags, they will take one or more of the below steps, commensurate with the degree of risk posed, to prevent and mitigate risk of identity theft. College personnel have the discretion to determine the degree of risk posed and to act accordingly.

a. Continue to monitor an account for evidence of identity theft;

b. Contact the person either by written notice or telephone;

c. Refuse to open a new account;

d. Close an existing account;

e. Reopen an account with a new number;

f. Notify the Director of Human Resources for determination of the appropriate step(s) to take based on the Oregon Identity Theft Act Best Practices; or

g. Determine that no response is warranted under the particular circumstances.

TBCC IDENTITY THEFT PREVENTION PROGRAM
ADMINISTRATIVE RULE NUMBER: B013
LAST APPROVED: April 01, 2013, January 15, 2015, February 2019
RELATED TO POLICY SERIES NUMBER: 212

SERVICE PROVIDER ARRANGEMENTS: B013.8

In the event the College engages a service provider to perform an activity in connection with a covered account, the College will take one of the following steps to ensure the service provider performs in accordance with the program:

A. Require, by contract, that service providers have appropriate policies and procedures in place designed to detect, prevent, and mitigate identity theft; or

B. Require, by contract, that service providers review this program and report any red flags to the Director of Human Resources; and

C. Require that contracts include indemnification provisions limiting the college's liability for the service provider's failure to detect, prevent, or mitigate identity theft.

NON-DISCLOSURE OF SPECIFIC PRACTICES: B013.9

Disclosure of specific information or practices regarding red flag identification, detection, mitigation and prevention practices may be limited to designated college staff and/or policymakers. Documents produced to develop or implement the program which describe specific practices may constitute security information and may be non-disclosable because disclosure would likely jeopardize the security of identifying information and may circumvent the college's identity theft prevention efforts.

A. The College completes an annual compliance evaluation in accordance with the Payment Card Industry (PCI) Security Standards Council.